CLASS SPECIFICATION
County of Fairfax, Virginia

CLASS CODE: 1832 **TITLE:** IT SECURITY PROGRAM DIRECTOR **GRADE:** S-33

DEFINITION:

Under the general direction of the Chief Information Officer and the Director of the Department of Information Technology, and under administrative supervision of the Director of the Department of Information Technology, directs and manages the County's information security program; ensures County's compliance with all federal and state information security regulations including homeland defense security initiatives; coordinates privacy and security requirements with HIPAA Compliance Manager to ensure integrity, sensitivity and confidentiality of data; provides architectural oversight, direction and recommendations for enterprise-wide information security technology; and performs other duties as required.

DISTINGUISHING CHARACTERISTICS OF THE CLASS:

This class is ultimately responsible for ensuring the security, integrity and confidentiality of the entire County government's information technology systems and data, to include the technical requirements for HIPAA. The HIPAA Compliance Manager differs from the Information Security Director in that the HIPAA Compliance Manager is responsible for developing and implementing privacy and security-related policies related to HIPAA law, concerning business practices and procedures limited to compliant use and access to medical records and related information.

ILLUSTRATIVE DUTIES:

Directs the development and enforcement of County-wide information security policies, standards, procedures and guidelines;
Advises Senior Management on matters related to IT security;
Collaborates with designated staff from Human Resources, County Attorney's office, Public Affairs, Senior Management and Public Safety agencies in oversight for enforcement of security violations;
Provides leadership (guidance and direction) while working with all facets of management within the County in developing secure and confidential technical solutions for business;
Develops and administers a County-wide information security awareness and education program;
Develops the proper selection criteria and evaluation process for the approval of all vendor products, tools and services related to the County's secure technology infrastructure;
Proactively protects the integrity, confidentiality and availability of the County's information resources, data and systems;
Establishes, manages and maintains organizational structures and communications channels with County Agency Information Security Coordinators as well as business partners of the County;
Represents the County's information security related interests at industry standards committee meetings and technical conferences;
Serves as liaison with Office of Homeland Security, Critical Infrastructure Protection Initiatives and Information Sharing and Analysis Centers (ISAC);
Develops action plans, schedules, budgets and condition reports and other top management communications tools intended to improve the status of information security in the County;

Investigates the ways that information security related technologies, requirements, statements, internal processes and organizational structures can be used to achieve the goals established by the Board, Executive Management, and the CIO.

Initiates and/or oversees the performance of periodic internal and third party risk assessments and audits that identify current and future security vulnerabilities, determines what level of risk is acceptable to management and identifies the best ways to reduce information security risks to the acceptable level;

Coordinates information security internal and external audits county-wide;

Provides technical expertise and guides the administration of security tools that control and monitor information security;

Participates in the development, implementation, and maintenance of effective disaster recovery plans, processes and procedures necessary to recover services in the event of a declared disaster; provides directions and consulting in these areas;

Provides post mortem analysis of information security breaches, violations, malicious activity and incidents to all levels of management;

Recommends corrective technical options and revisions to IT security initiatives and policies to prevent future occurrences; and

Supervises and trains County information technology security office staff.

REQUIRED KNOWLEDGE, SKILLS AND ABILITIES:

Thorough knowledge of data security and access control systems, encryption, and related matters;

Thorough knowledge of communications protocols and standards related to the security of information systems;

Ability to establish and maintain an effective program to identify potential security breaches and implement counter measures;

Thorough knowledge of server administration as applied to network and internet security;

Considerable knowledge of effective supervisory methods, practices, and techniques;

Ability to plan, organize, coordinate, assign, and evaluate the work of subordinate staff;

Ability to interface with individuals at all levels of the organization and establish effective working relationships with other staff and vendors;

Ability to develop, maintain and work in a secured environment with confidential information;

Ability to communicate effectively, both orally and in writing;

Ability to provide training and technical assistance to less experienced staff.

EMPLOYMENT STANDARDS:

Any combination of education, experience, and training equivalent to the following:

Graduation from an accredited four-year college or university with a bachelor’s degree in electrical engineering, computer science or telecommunications management; PLUS

Five years’ information security systems experience, including supervisory experience.

CERTIFICATES AND LICENSES REQUIRED:

None.

REGRADED/REVISED: February 26, 2004
ESTABLISHED: May 24, 1999